REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
May 1990	Conference paper	

4. TITLE AND SUBTITLE

See report.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

See report.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

See report.

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

See report.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A - Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Presented at the IEEE 1990 National Aerospace and Electronics Conference (NAECON 1990) held in Dayton, Ohio, on 21-25 May 1990.

14. ABSTRACT

See report.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU		**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			

JIAWG DIAGNOSTIC CONCEPT AND COMMONALITY REQUIREMENTS

Richard S. Mejzak
Tactical Air Department
Naval Air Development Center
Warminster, PA

ABSTRACT

One of the major Joint Integrated Avionics Working Group (JIAWG) objectives is to ensure that reliable and maintainable systems can be built from JIAWG common modules. To facilitate attaining this objective, a JIAWG Diagnostic Concept and Initiative are discussed. A three-level diagnostic concept is described in terms of system, system element, and module management requirements. The corresponding JIAWG initiative is also discussed with respect to requirements for developing a common methodology for deriving fault coverage metrics as well as proof of concept demonstrations necessary to show compliance with JIAWG requirements.

BACKGROUND

The JIAWG A^3 (Advanced Avionics Architecture) Standard[1] was prepared for the Advanced Tactical Fighter (ATF), Advanced Tactical Aircraft (A-12), and the Light Helicopter (LHX) in accordance with the Joint Integrated Avionics Plan[2] (JIAP). This standard is also intended to describe common avionics functional building blocks, developmental guidelines, and integration techniques suitable for a broad range of future avionics developments. The general A^3 hierarchical structure is depicted in Figure 1. Specific requirements addressed in the A3 Standard include system partitioning, system interconnects, interoperability, exchangeability, certification, information security, system fault management and diagnostics, system initialization, software requirements, technology insertion, and airframe integration. This paper focuses on the system fault management and diagnostic requirements of the A^3 Standard.

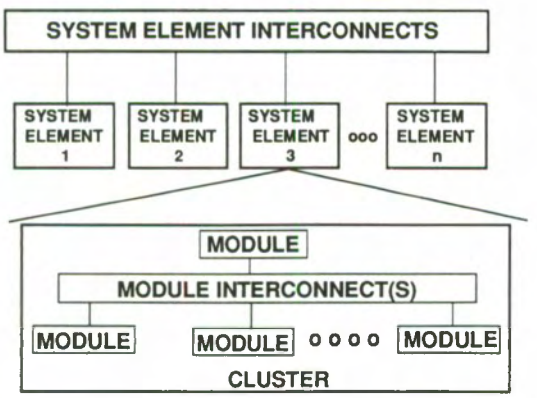


Figure 1. A^3 Hierarchical Structure

JIAWG SYSTEM FAULT MANAGEMENT AND DIAGNOSTIC REQUIREMENTS

The A^3 standard specifies that the system shall perform fault detection, fault containment, fault isolation, and fault recovery as well as record faults for post-mission analysis and maintenance. Although there are a number of candidate fault tolerance approaches[3] for achieving these requirements, it is not the intent of the A^3 Standard to specify design techniques. However, it is important to note that all elements (fault detection, containment, isolation, and recovery) must be present in a system design to realize any type of fault tolerance scheme. For clarity, these terms are defined below[4]:

> Fault Detection - Hardware and software mechanisms used to determine if a fault exists;
>
> Fault Containment - Techniques used to prevent fault-damaged information from propagating through a system after a fault occurs but before it is detected;
>
> Fault Isolation - hardware and software techniques to diagnose and locate a fault; and
>
> Fault Recovery - mechanisms to correct the fault by voting out incorrect results, replacing faulty components with spares, or configuring to a degraded or alternate mode of operation.

The objectives of the JIAWG system fault management and diagnostic requirements are to ensure that provisions are being incorporated in the design to support full mission operational and maintenance requirements within the A^3 philosophy. It should be noted, however, that the A^3 philosophy requires the use of common modules procured from different vendors. This demands that fault coverage metrics and capabilities are consistent at the the module level so that reliability requirements can be satisfied at the system level. To be consistent at the module level, necessitates a common methodology for deriving

and verifying metrics.

Trades for enhancing system reliability requirements involve balancing component reliability with fault tolerance and graceful degradation options. The ability to incorporate fault tolerance and graceful degradation is totally dependent on the quality of the diagnostics provided.

Therefore, the A3 Standard includes requirements to facilitate and verify these objectives.

JIAWG DIAGNOSTIC CONCEPT

The JIAWG diagnostic concept consists of three distinct management levels as depicted in Figure 2. A top-down hierarchical concept is shown which consists of system, system element, and module management levels. The management responsibilities of each level are provided in Figure 2 and described in the following paragraphs.

System Management

The system level is responsible for detecting, containing, and isolating faults down to the system element level. If a functionally equivalent spare system element is available, system reconfiguration consists of switching in a spare system element. Otherwise, system reconfiguration consists of configuring to a degraded mode option. Status is then logged to record the particular action taken. It should be noted that degraded mode reconfiguration is only managed by the system level.

System Element Management

The system element level is responsible for detecting, containing, and isolating faults down to the module level. If a functionally equivalent spare module is available, system element reconfiguration consists of switching in a spare module. Otherwise, the system element is declared failed. Status is then logged and reported to the system level.

Module Management

A module is assumed to be partitioned into functional areas as a convenient means of identifying a component or group of components. The module level is responsible for detecting, containing, and isolating faults down to the functional area. If a functionally equivalent spare functional area is available, module reconfiguration consists of switching in a spare functional area. Otherwise, the module is considered failed. Status is then logged on the module and reported to the system element manager.

JIAWG COMMON DIAGNOSTIC REQUIREMENTS

It is envisioned that use of the following would be required to achieve a common JIAWG

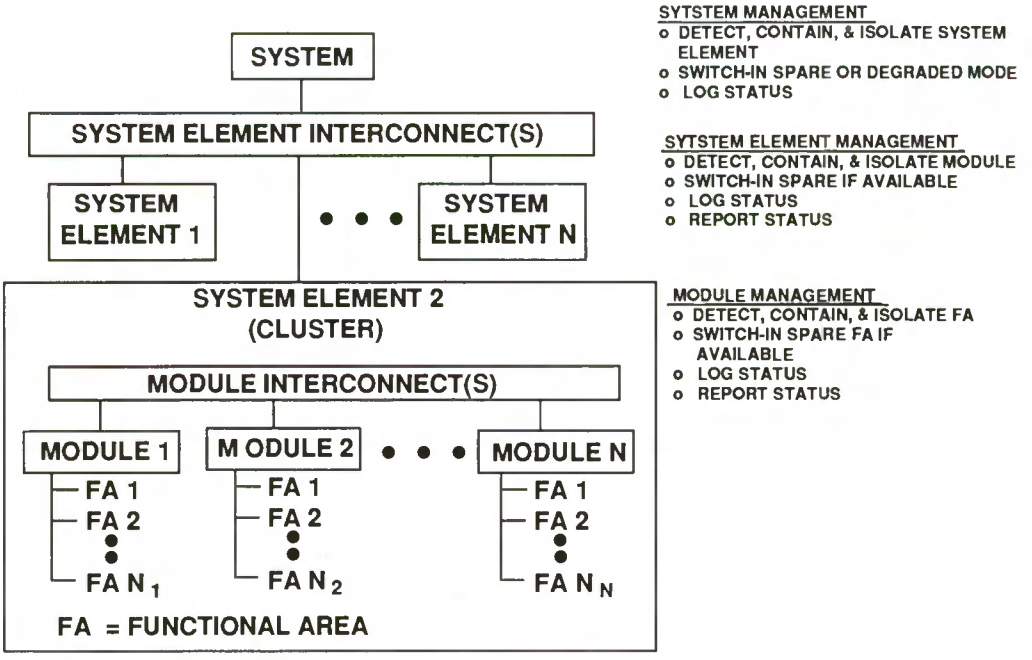


Figure 2. JIAWG Diagnostic Concept

Diagnostic and Fault Management Concept.

o Common methodology for deriving and verifying fault coverage metrics;

o Common fault log information, reporting, and interpretation; and

o Common Test/Maintenance (TM) bus interface and command set. (The TM bus is a serial path specified by JIAWG for test and maintenance control and data communications within a system element).

To ensure that these requirements are being properly addressed, a Diagnostic Initiative is being proposed by JIAWG.

JIAWG DIAGNOSTIC INITIATIVE

Using the JIAWG common diagnostic requirements as a baseline, numerous meetings were held with tri-Service and industry representatives to ensure that the correct requirements for the Diagnostic Initiative are being addressed. The results of a concensus indicates that the focus of the initiative is correct but should account for the fact that various JIAWG groups are already specifying module fault log requirements as well as a common TM bus command set. Taking this into consideration resulted in the requirements for two basic products for the Diagnostic Initiative. These products are:

1. Common methodology for deriving fault coverage metrics and

2. Methodology for demonstrating system level diagnostics using the JIAWG specified module fault logs and common TM bus command set.

Although the details of the tasks and deliverables associated with these requirements are still being formulated, the following paragraphs discuss their possible implications.

Common Methodology for Deriving Fault Coverage Metrics and Verifying Module Level Diagnostic Compliance

A concept for a module fault coverage methodology is shown in Figure 3. It is anticipated that this would consist of a combination of common procedures and tools to facilitate the methodology. As shown in Figure 3, fault metrics would be derived and verified by use of design unique gate level models which would then be compared to JIAWG specified values to verify compliance. It should be noted that it is necessary to use high fidelity gate level models so that there is sufficient confidence that the specified requirements are met. The methodology would also require the use of tools such as a fault list, optimized test vectors, insertion mechanism, and comparison mechanism.

Methodology for Verifying System Level Diagnostic Compliance

Demonstrating system level compliance requires exercising the system, system element, and module management levels shown in Figure 2. However, all capabilities are rooted in the module diagnostic capabilities and the ability to communicate this information to higher levels in the system. It should be noted that in an

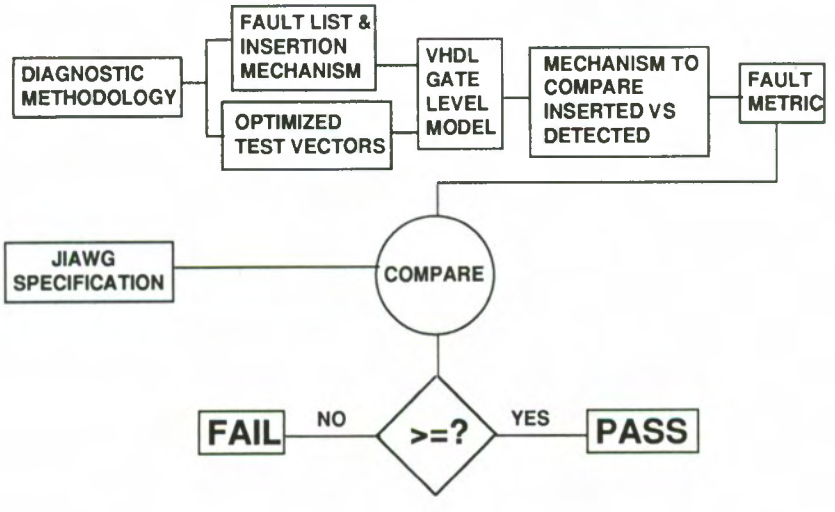


Figure 3. Fault Coverage Methodology Concept

operational environment, GO/NO-GO type information is used and in a depot maintenance environment, fault log information is used. However, to enable deriving the necessary information for both operational and maintenance purposes requires an effective module partitioning and fault log scheme. A possible module partitioning and fault log scheme is shown in Figure 4. As indicated previously, the module is partitioned into functional areas as a convenient means of identifying a component or group of components. This partitioning could also provide more visibility when exploring on-module redundancy opportunities to achieve higher levels of reliability as well as fault detection schemes using voting techniques.

The types of evaluations that could be performed on modules from a systems point of view would include the ability to:

Detect and isolate to a functional area to demonstrate the effectiveness of the partitioning;

Switch in a spare functional area if available to demonstrate the use of on-module redundancy;

Log status to demonstrate manner of recording fault information in the fault log;

Communicate fault information over TM bus to demonstrate use of a common interface and command set to include the following:

o In an operational environment, information would include GO/NO-GO and other TBD information to the system element manager and

o In a depot maintenance environment, functional area status information would be read from the fault logs; and

Communicate fault information over other module and system level interconnects to demonstrate system level fault management.

SUMMARY

A fault management and diagnostic concept as contained in the JIAWG A3 Standard was discussed along with the requirements and objectives for a diagnostic initiative which is designed to facilitate the realization of these requirements. Details regarding tasks and deliverables for the Diagnostic Initiative statement of work are currently being developed by a JIAWG tri-Service committee.

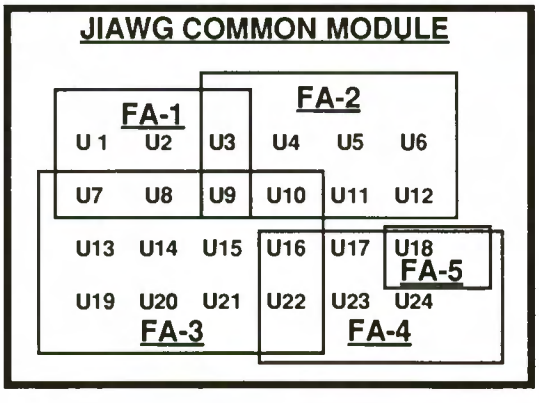
REFERENCES

1. "Joint Integrated Avionics Working Group Advanced Avionics Architecture (A3) Standard", J87-01, December 1989

2. "Joint Integrated Avionics Plan for New Aircraft", Department of Defense, March 1989

3. Siewiorek, D.P., and Swarz, R.S., "The Theory and Practice of Reliable System Design", Digital Press, Bedford Massachusetts, 1982

4 Rennels, David, A., "Distributed Fault-Tolerant Computer Systems", Computer, March 1980



FAULT LOG

CMPT	FA 1	2	3	4	5
U1	X				
U2	X				
U3	X	X			
U4		X			
U5		X			
U6		X			
o					
o					
U15			X		
U16			X	X	
U7				X	
U18				X	X
U9			X		
o					
o					
U24				X	

Figure 4. Possible Module Partitioning and Fault Log